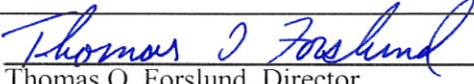


Thomas. O Forslund, Director

Governor Matthew H. Mead

<b>Policy Title:</b>	Mobile Devices	
<b>Policy Number:</b>	S-022	
<b>Effective Date:</b>	July 1, 2013	
<b>Approval:</b>	 Thomas O. Forslund, Director	<u>5/21/13</u> Date

**Purpose:**

This policy establishes the requirements for mobile devices to synchronize to a system containing Wyoming Department of Health (WDH) data.

**Scope:**

This policy applies to all WDH workforce.

**Definitions:**

*Mobile Device* means portable cartridge/disk-based, removable storage media or a portable computing and communications device with information storage capability.

**Policy:**

1. **General.** To ensure standardized controls are enabled, mobile devices of all types shall be issued by a delegated WDH fiscal manager or designee. Devices purchased for business purposes by WDH workforce are discouraged, but not prohibited. Individual purchases shall be approved in advance in accordance with WDH Policy S-010; Physical Security, and under the condition that once a mobile device syncs with any WDH system, it is no longer a personal device, and is subject to this policy.
  - a. E-mail enabled devices are allowed as a supplementary delivery method.
  - b. All data transferred from the WDH network and applications remain the property of WDH.
  - c. Mobile storage is intended for a limited timeframe only as end users move between work locations. Protected health information (PHI) shall be erased as soon as possible.
  - d. End users shall take reasonable steps to prevent the loss or theft of the device.
  - e. Loss or theft of a device shall be reported to the WDH Compliance Office and the Department of Enterprise Technology Services (ETS) Security Officer within 24 hours.
  - f. In the event of loss or theft, remote kill software shall be used to destroy all data on a mobile device containing PHI.
2. **User responsibilities**
  - a. Lost or stolen mobile computing and storage devices shall be reported in accordance with WDH Policy AS-009 and S-006a; Report and Response to Privacy Violations and Security Incidents.
  - b. Access to mobile devices which store or transmit sensitive information, or which can be used to connect to other systems shall be authenticated.
  - c. Passwords/PINs shall be changed and maintained in accordance with WDH Policy S-005d; Password Use and Management.
  - d. Mobile Devices synchronizing to Google Apps shall meet the requirements of ETS Policy 10200-P020: Use of Mobile Devices for Synchronizing to Google Apps.

- e. Any WDH workforce member using a personal mobile device to synchronize with the State's Google Apps domain shall complete a Use of Non-State Owned Mobile Device for Synchronizing with State of Wyoming Google Apps User Agreement.
- f. The Division Administrator shall provide written authorization before e-mail or other repositories containing PHI is downloaded to mobile computing or storage devices.
- g. PHI stored on lap or other mobile devices shall be protected against unauthorized access and disclosure via encryption or other appropriate measures.
- h. WDH workforce members using a mobile device shall ensure the data maintained on the device is backed up on a regular basis.
- i. WDH workforce members shall limit the device to only necessary applications and services.
- j. Use of mobile devices outside WDH poses risks to the devices and the information contained therein. Therefore, lap and other mobile devices shall use antivirus and personal firewall software when connected to any network other than WDH.

**3. Administrators, fiscal managers, or designee**

- a. A delegated fiscal manager shall keep an inventory of the allocation of all mobile devices, including those which store PHI, and the personnel who use them.
- b. Division Administrators shall approve all new mobile computing and storage devices that connect to any WDH information system.
- c. Any non-WDH-owned device that connects to a WDH information system or network shall first be approved and inventoried prior to use.
- d. Mobile devices containing PHI shall have the ability to remotely disable and/or destroy information.

**Contacts:**

De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664  
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

**Forms:**

Use of Non-State Owned Mobile Device for Synchronizing with State of Wyoming Google Apps User Agreement

**Policies:**

AS-009 and S-006a; Report and Response to Privacy Violations and Security Incidents  
S-005d; Password Use and Management  
S-010; Physical Security

**References:**

45 CFR §§ 164.306-312  
NIST SP-800-53

**Training:**